U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Patent Capture and Application Processing System – Initial Processing (PCAPS-IP)

PTOP-006-00

March 4, 2010

Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is a requirement of the Privacy Act of 1987 and OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.* A PIA documents the due diligence and oversight placed upon information associated with the project or system in question. Written from the System Owner's perspective for the American public, the PIA discloses what information is being collected, and how that information is protected. The intent is to build confidence that privacy information is secure, processes that utilize this information comply with Federal requirements, and more importantly, inform the privacy expectations of the American public.

The Privacy Threshold Analysis (PTA) is a separate artifact that must be completed prior to beginning this PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

Patent Capture and Application Processing System–Initial Processing (PCAPS-IP)

The Patent Capture and Application Processing System – Initial Processing (PCAPS-IP) provides multiple applications that allow the submission, categorization, metadata capture, and Patent examiner assignment of Patent applications from internal and external customers of the USPTO. It supports the Patent Business Function of USPTO.

PCAPS-IP resides within the USPTO Data Center Located on the third floor of Madison East Facility, 600 Dulany Street, Alexandria, Virginia 22314.

The PCAPS-IP is a Major Application (MA) that provides the following services or functions in support of the USPTO mission:

Application Routing Tool (ART)

ART is an automated patent application processing support system that provides a suggested routing location for new patent applications that have been successfully scanned into the PASS database. ART uses the Bibliographic Retrieval Service (BRS) Query by Example (QBE) technology to provide a recommended GAU location, class, and subclass for routing pending patent applications that have been successfully scanned into the PASS database. For each application, ART searches the text of the background, summary of the invention, and abstract for certain keywords and compares the frequency of those keywords to existing published patents. A score is generated, by classification, for number of times the keywords are found within an application that were also found in published patents. The classification with the highest number of hits is used to determine a tentative classification for routing.

ART System Access Groups

Access Group(s)	User Information	Approximate Number of Users
Primary Classifiers/ Routers	USPTO employees	300
USPTO Supervisory Patent Examiner (SPEs)	USPTO employees	300-500
Office of Initial Patent Examination (OIPE)	USPTO employees	1-3
USPTO System Development/Maintenance Managers, Developers	ART Project Team/Contractors	30
SIRA Managers	SIRA	4

Checker (Checker)

The Checker self-contained downloadable application is a state-of the-art Microsoft (MS) Windows software program employing a logical and intuitive user interface to validate and convert patent applications to be compliant with 37 Code of Federal Regulations (CFR) 1.821 – 1.825 for both 'old rules' (October 1990) and 'new rules' (July 1998). Checker contains a setup executable (.exe) to install the application. Checker is a stand-alone application and does not facilitate the delivery of patent applications to the USPTO. In addition, Checker does not connect to USPTO. The Checker application runs locally on the user's personal computer. Checker replaces the previous DOS-based versions of Computer Readable Format (CRF) and Checker. Checker is available to the public as a download from the USPTO website for MS Windows Operating System (OS) personal computers.

Checker System Access Groups

Access Group(s)	User Information	Approximate Number of Users
Patent applicants	Public access	Not Applicable

Enterprise Application Integration (EAI) Hub - (EAI Hub)

The EAI Hub framework is a scalable, robust, and extensible system that enables the USPTO to model and automate business processes at the enterprise level. The EAI Hub system supports the key functions of asynchronous message routing, data transformation, data types-transformation, message filtering and restructuring to fit the needs of various applications, and data format conversions for Extensible Markup Language (XML), PDF, and Tagged Image File Format (TIFF).

EAI Hub System Access Groups

Access Group(s)	User Information	Approximate Number of Users
Patent Applicant	No	Unlimited

Electronic Filing System - WEB (EFS-Web)

EFS-Web is a system that provides a simple, safe, and secure method for e-filers to submit patent application documents as PDF files over the Internet to the USPTO. EFS-Web utilizes the existing USPTO Portal Infrastructure. EFS-Web allows applicants, or their legal representatives, to submit patent applications in electronic form and eliminate traditional paper processes. EFS-Web has increased e-file adoption rates and simplifies processing of applications.

EFS-Web System Access Groups

Access Group(s)	User Information	Approximate Number of Users
Patent Applicants – Registered (Requires x.509 digital certificate authentication (PKI))	Public access	>20000
Patent Applicants – Unregistered (TLS)	Public access	N/A
Office of Initial Patent Examination	N/A	10

Patent Application Services and Security (PASS)

The PASS system provides the capability to use electronic images of patent applications to support USPTO operations. The PASS system was previously identified as Patent Application Capture and Review (PACR). PASS supports two user groups: the Office of Initial Patent Examination (OIPE) and the Licensing and Review (L&R) Group. PASS provided OCR, data extraction and verification, security screening, and application viewing, DTSA CD generation, PGPub, Grant tape publication, and East Data Center (EDC) exports.

PASS System Access Groups

Access Group(s)	User Information	Approximate Number of Users
OACP/OIPE	No	90
OACP/L&R	No	30
Administrators	PASS Administrators	-

PatentIn

PatentIn is a self contained downloadable application that allows patent applicants to generate nucleic and amino acid sequence listings. PatentIn provides automated validation and error checking mechanisms. This enables users to use a sequence editor to enter or import existing sequences manually, while configuring each sequence according to a specific feature attribute. The application fully complies with World Intellectual Property Organization (WIPO) Standard ST.25 Sequence Listing Requirements. The PatentIn system was designed for use by the general public and is not used internally by the USPTO. PatentIn is downloaded from the public USPTO Web server and installed on personal computers running the MS Windows OS. The user generates output files containing sequence listings that can be submitted with a patent application. PatentIn is a stand-alone application and does not facilitate the delivery of sequence listings to the USPTO. In addition, PatentIn does not connect to USPTO. The PatentIn application runs locally on the user's personal computer.

PatentIn System Access Groups

Access Group(s)	User Information	Approximate Number of Users
Patent Applicant	Public access	Not Applicable

Patent Application Location Monitoring Pre Examination (PALM Pre-Exam)

The PALM Pre-Exam, as identified as PALM Pre-Ex, system supports the prosecution and related administrative functions of a patent application through its life cycle; and also tracks, monitors, and reports on the prosecution status of patent applications. PALM Pre-Exam supports the processing of over 350,000 applications each year. PALM serves the needs of over 5,000 Office of Patents staff, including over 3,700 members of the patent examining corps. The examining corps processes over twelve million transactions per month in addition to Web-based queries and batch processing.

PALM Pre-Exam System Access Groups

Access Group(s)	User Information	Approximate Number of Users
OIPE	USPTO Employees	150
Patent Examiners	USPTO Employees	100
PGPub Users	USPTO Employees	40
RTIS Contractors	Contractors	50
Re-Exam Users	USPTO Employees	15

Patent Application Location Monitoring Patent Cooperation Treaty Operations System (PCT Ops)

The PCT Ops, also referred as PCT Operations Workflow and Electronic Review System (POWER), system is a USPTO Automated Information System (AIS) designed to support an automated, workflow-driven, client-server environment that support Patent Cooperation Treaty (PCT) patent application functions. PCT Ops works with an electronic application in an integrated desktop environment. The PCT Ops system minimizes the movement of paper through the United States Receiving Office (RO/US) processing stream and automates the application filing process under Chapter I and Chapter II of the PCT. The PCT Ops system supports the initial receipt of an application or later-submitted papers, review of the application by PCT personnel, generation of outgoing correspondence, and tracking of the application while it is being processed by RO/US. Case files ultimately provide information in an electronic medium that facilitates exchange with PCT Operations' principal internal customer, the USPTO Examining Corps, as well as with the WIO, Trilateral Office partners, and the other international partners of USPTO.

PCT Ops System Access Groups

Access Group(s)	User Information	Approximate Number of Users
Patent Office (PCT Legal, PASS, Supervisors)	USPTO Employees	150
PCTBDE (user directly enters data – authenticated via Lightweight Directory Access Protocol (LDAP))	USPTO Employees	20
Administrators	PCT Ops Admin	-

Patent Application Location Monitoring - Reporting System (PRS)

The PRS produces many productivity and statistical reports that are crucial to the Patents Corps business operation. The PRS processes and delivers reports to Patents Corp, supporting various PALM subsystems and business areas, including: PALM-EXPO, Pre-Exam, File Ordering System (FOS), Infrastructure, and PCT Ops. These reports are available via the USPTO Intranet on-line and on-demand to over 5,000 Examiners, Directors, Supervisory Patent Examiners (SPEs), and Clerical staff. The reports are delivered via different means. Static reports are made available electronically on the Web. Dynamic reports are accessible via the USPTO intranet (online) and allow real-time database access for most up-to-date information via the Web; and report distribution via email. PRS provides PALM users (over 7000 examiners, 500 managers, and over 100 other users) with access to PALM data via a COTS reporting platform. Most of the reports obtain data from a daily snapshot of the PALM on-line system. The reports can be scheduled to run at a predefined time or display data instantaneously. The scheduled reports are archived. Access to archive and inputs for instantaneous reports are provided via a USPTO Intranet website.

PRS Access Groups

Access Group(s)	User Information	Approximate Number of Users
Patent Examiners	USPTO Employees	7000
Special Patent Examiners	USPTO Employees	500
Directors and Analysts	USPTO Employees	70-100

QUESTIONNAIRE

1. What information is collected (e.g., nature and source)?

   PCAPS-IP collects information from patent applicants (inventors) or their legal representative as part of the patent application submission process. Information from the applicant must be submitted on the patent application form either electronically or in paper copy. PCAPS-IP contains information provided as part of the patent application, which includes; full name, address, phone number, email address, and citizenship status of patent applicant (inventor). Additional information is collected for each additional inventory, company, Legal Representative under 35 U.S.C. 117, or Party of Interest under the authority of 35 U.S.C. 118.

2. Why is this information being collected (e.g., to determine eligibility)?

   Information is collected to facilitate the issuing of a U.S. patent to the inventor (patent applicant). This collection of information is required by 37 CFR 1.76. The information is required for members of the public to file a patent application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14.

3. What is the intended use of information (e.g., to verify existing data)?

   Information is collected to issue a U.S. patent to the inventor (patent applicant). Once the application is published, the patent is released to the public, unless otherwise requested by the patent applicant at the time of submission. This information is also used to construct a unique name (distinguished name) and to communicate with user about the certificate grant and software distribution process.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

   Information collected remains confidential until the patent application is published. Once published, information is publicly released. Information may be shared with the following:

   a. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

   b. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

c. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

d. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information are be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

e. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

f. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

g. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure will be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure will not be used to make determinations about individuals.

h. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

i. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

Privacy information is required for the processing of Patents within the PCAPS-IP system. Members of the public voluntarily provide the information. As part of the patent application process, individuals consent to providing this information for the primary purpose of processing and/or examining the submission related to a patent application or patent. All applicants are notified that this submission is voluntary. However, the applicant is notified that if the information is not provided then USPTO may not be able to process and/or examine the patent application submission.

6. How will the information be secured (e.g., administrative and technological controls)?

   Information is protected in PCAPS-IP through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, VPN, and encryption, where required. PCAPS-IP adheres to the principles of least privilege, least functionality. In addition, PCAPS-IP utilizes secure authentication via username and password credentials. Electronic patent application (e-filer) transmissions from patent applicants are encrypted via a secure HTTPS (SSL/TLS) and Public Key Infrastructure (PKI) x.509 digital certificates. Digital certificates are utilized to authenticate patent applicants or their legal representatives, where required for access to PCAPS-IP information.

Management Controls:

1. The USPTO uses the Life Cycle review process to ensure that management controls are in place for the PCAPS-IP system. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address the management, operational, and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency check on all personnel, including contractor staff.
2. The USPTO Personally Identifiable Data Extracts Policy (DRAFT)

Operational Controls:

3. Automated operational controls include securing all hardware associated with the PCAPS-IP System in the USPTO Data Center. The Data Center is controlled by access card entry and is manned by a uniformed guard service to restrict access to the servers, their operating systems, and databases. Contingency planning has been prepared for the data. Backups are performed on the processing data bases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database UserID; (4) Restricted data display, as required; and (5) Restricted access.
4. Manual procedures will be followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:

    a. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.

b. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.

c. Obtain management concurrence in the log, if an extract aged over 90 days is still required.

d. Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO VPN.

e. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

f. Encrypt and password-protect prior to transmission any sensitive PII data extracts that are sent to an external email address via the Internet. The password key should be forwarded to the recipient in a separate email from the attached file.

7. How will the data extract log and verify requirement be met?

USPTO has not developed a centralized logging system for PII data extracts. Such a system would track the following categories of information:

a. Who performed the extract,

b. When extract was done,

c. What was the extract,

d. Where was the extract taken from,

e. Has the extract been deleted and,

f. If not deleted after 90 days, to monitor that it is still needed in 90 day intervals.

Until a system is implemented, USPTO is using the following compensating controls to protect PII data:

a. No extracts of sensitive data may be copied on to portable media without a waiver approved by the DoC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.

b. All laptop computers allowed to store sensitive data must have full disk encryption.

c. All remote access to public USPTO systems containing sensitive data must be encrypted. All remote access to internal USPTO systems containing sensitive data must fully comply with DoC Remote Access Policy requirements.

d. All flexiplace/telework agreements for working off site require that adequate data protection be in place.

8. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

   A system of records exists for Patent Application Files and USPTO PKI Registration and Maintenance System.
   Source: http://www.uspto.gov/web/doc/privacy_sorn.htm
   Application Data Sheet 37 CFR 1.76, PTO/SB/14 (07-07), Approved for use through 06/30/2010. OMB 0651-0032, U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE, http://www.uspto.gov/ebc/portal/efs/sb0014_fill.pdf, http://www.uspto.gov/ebc/portal/privacy.htm, and Certificate Action Form, http://www.uspto.gov/ebc/documents/certificateactionform.pdf

9. Are these records covered by a record control schedule approved by the National Archives and Records Administration (NARA)?

No. GRC 20 allows agency determination that certain electronic records are authorized for erasure or deletion when they are no longer needed for administrative, legal, audit, or other operational purposes. Electronic records that represent hard copy records can be deleted after expiration of the retention period authorized for the hard copy records.

SIGNATORY AUTHORITY

Agreed: /s/ William Stryjewski _____ 3/11/2010 _____/_____/_____

William Stryjewski — Date

Information System Owner

Agreed: /s/ Rod Turk _____ 3/11/2010 _____/_____/_____

Rod Turk — Date

Senior Agency Information Security Officer

Agreed: _____ _____/_____/_____

John B. Owens II — Date

Chief Information Officer